

U.S. Serial No. 09/746,325

Page 2

## REMARKS

In response to the Final Office Action mailed on December 1, 2005, Applicant respectfully requests reconsideration based on the following remarks. Applicant respectfully submits that the claims as previously presented are in condition for allowance.

Claim Rejections Under 35 U.S.C. § 103(a)

Claims 1-4, 6-10, and 12-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Microsoft Passport in view of U.S. Patent No. 5,966,705 issued to Koneru et al. (hereinafter "Koneru").

For an obviousness rejection to be proper, the Examiner must meet the burden of establishing that all elements of the invention are disclosed in the prior art; that the prior art relied upon, coupled with knowledge generally available in the art at the time of the invention, must contain some suggestion or incentive that would have motivated the skilled artisan to modify a reference or combined references; and that the proposed modification of the prior art must have had a reasonable expectation of success, determined from the vantage point of the skilled artisan at the time the invention was made. *In re Fine*, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988); *In Re Wilson*, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970).

This rejection is respectfully traversed because Microsoft Passport in view of Koneru does not teach or suggest all of the elements in Claims 1-4, 6-10, and 12-23.

Claim 1 recites "A method for providing information on a plurality of users to a plurality of requestors over the Internet, comprising: storing information on the plurality of users in a database located on a cookie management system and associating the information with a plurality of keys; receiving a request at the cookie management system for information on a particular user from a requestor over the Internet; receiving both a user-supplied password and a key associated with the request at the cookie management system from the requestor over the Internet, the key associated with the request included in a cookie on a machine of the particular user, wherein the key associated with the request is retrieved from the machine of the particular user by the requestor, and wherein the user-supplied password is obtained from the particular

36968/248469

U.S. Serial No. 09/746,325

Page 3

user by the requestor and grants the requestor permission to use the information on the particular user in the cookie management system; using both the user-supplied password and the key associated with the request to retrieve the information on the particular user from the database; and forwarding the information on the particular user to the requestor over the Internet.” (Emphasis added.)

In Claim 1, the user-supplied password is the password that a particular user chooses, while the keys associated with the information is the key that is associated with the user's information when the information is stored in a database on the cookie management system. Therefore the user-supplied password and the keys are different from each other. The Examiner however, treats both the keys and the user-supplied password as the same, i.e., “Passports”. Although a subtitle “use of cookies”, on Examiner numbered page 15 of Microsoft Passport discusses the use of cookies, the Microsoft Passport does not teach or suggest the keys associated with the user's information. All the Microsoft Passport discloses is that the Passport site stores a user's member name, the time the user signed in, and the user's profile information in a secure, encrypted cookie on the user's hard disk. Therefore, Microsoft Passport fails to teach or suggest the element “receiving both a user-supplied password and a key associated with the request at the cookie management system from the requestor over the Internet”, as recited in Claim 1.

Microsoft Passport teaches that a user creates a Passport; that the user's information is securely sent to the Passport site; and that the user's information stored in the Passport is transferred to other services when the information is in the public Profile. Microsoft Passport however, does not teach or suggest how the user's information is disclosed in response to the request and how both the keys and the password are used by the requestor to request the user's information. Therefore, Microsoft Passport fails to teach or suggest the elements “the key associated with the request is retrieved from the machine of the particular user by the requestor; and the user-supplied password is obtained from the particular user by the requestor and grants the requestor permission to use the information on the particular user in the cookie management system”, as recited in Claim 1.

Col. 2, lines 49-52 of Koneru teach that the user is assigned a token, such as a GUID, that uniquely represents the user; and that the token is used as a key to a database entry associated

36968/248469

U.S. Serial No. 09/746,325

Page 4

with the user on the site. Col. 2, lines 60-62 of Koneru also teach that using the user identification as a key, only one database entry is needed to track users across both non-secure and secure areas. Thus, the key, as disclosed in Koneru, is only for identifying the user across both non-secure and secure areas, rather than for letting the requestor request the information. Koneru is also silent in associating the key with the user's information or receiving or granting the requestor permission to the user's information by using the user's password.

Therefore, Koneru does not teach or suggest the element "the key associated with the request is retrieved from the machine of the particular user by the requestor; and the user-supplied password is obtained from the particular user by the requestor and grants the requestor permission to use the information on the particular user in the cookie management system", as recited in Claim 1.

As stated above, Microsoft Passport is related to creating a Passport in response to the user's information. Koneru is related to tracking a user across secure and non-secure areas on a computer network. Thus, neither of them is related to receiving a request from a requestor, which is not the user, for the user's information. Therefore, one of ordinary skill in the art at the time of invention by Application would not be motivated to combine Microsoft Passport with Koneru to arrive at the subject matter recited in Claim 1. Even if Microsoft Passport is combined with Koneru, the combination does not render Claim 1 obvious because it fails to teach or suggest at least the element "the key associated with the request is retrieved from the machine of the particular user by the requestor; and the user-supplied password is obtained from the particular user by the requestor and grants the requestor permission to use the information on the particular user in the cookie management system", as recited in Claim 1.

For at least the above reasons, Claim 1 is patentable over Microsoft Passport in view of Koneru. Because they depend from Claim 1, Claims 2-4, 6-8, 14, and 21 are also patentable over Microsoft Passport in view of Koneru.

Claim 9 recites "receiving a user-supplied password from a user to the requestor website, the password granting the requestor website permission to use information on the user in a cookie management system; sending a query over the Internet from the requestor website to the cookie

36968/248469

U.S. Serial No. 09/746,325

Page 5

management system for data associated with the key, the query including both the key retrieved from the cookie and the user-supplied password"; and Claim 16 recites "a cookie management system for receiving a request over the Internet from a requestor for information on a particular user, the request including both a user-supplied password and a key stored as part of a cookie on a machine of the particular user, wherein the key associated with the request is retrieved from the machine of the particular user by the requestor, and wherein the user-supplied password is obtained from the particular user by the requestor and grants the requestor permission to use the information on the particular user at the cookie management system".

Because Claims 9 and 16 include elements that are similar to Claim 1, Claims 9 and 16 are patentable over Microsoft Passport in view of Koneru for at least the same reasons that Claim 1 is patentable over Microsoft Passport in view of Koneru. Because they depend from Claim 9, Claims 10, 12-15, and 22 are patentable over Microsoft Passport in view of Koneru for at least the same reasons advanced with respect to Claim 9. Because they depend from Claim 16, Claims 17-20, and 23 are patentable over Microsoft Passport in view of Koneru for at least the same reasons advanced with respect to Claim 16.

36968/248469

PAGE 7/8 \* RCVD AT 2/28/2006 3:28:34 PM [Eastern Standard Time] \* SVR:USPTO-EFAX-2/0 \* DNIS:2738300 \* CSID:8602860115 \* DURATION (mm-ss):02-28

**BEST AVAILABLE COPY**

U.S. Serial No. 09/746,325

Page 6


Conclusion

In view of the foregoing remarks, Applicant submits that the above-identified application is in condition for allowance. Early notification to this effect is respectfully requested.

If any issues remain, the Examiner is invited to contact the undersigned at the telephone number below.

If there are any charges with respect to this response or otherwise, please charge them to Deposit Account 06-1130 maintained by Applicants' attorneys.

Respectfully submitted,

By   
Anne Davis Barry  
Registration No. 47,408  
Customer No. 36192

Date: February 28, 2006  
Address: 55 Griffin Road South, Bloomfield, CT 06002  
Telephone: (860) 286-2929

36963/248469

PAGE 8/8 \* RCVD AT 2/28/2006 3:28:34 PM [Eastern Standard Time] \* SVR:USPTO-EFXRF-2/0 \* DNIS:2738300 \* CSID:8602860115 \* DURATION (mm-ss):02-28

BEST AVAILABLE COPY